情報セキュリティに関する特記仕様書

１　法令順守

以下のものを順守しなければならない。

(1) 個人情報の保護に関する法律

(2) 行政手続における特定の個人を識別するための番号の利用等に関する法律

(3) 関係法令

(4) 本市の条例、規則

(5) 特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）

(6) 茨木市個人情報の適正な取扱いに関する基本方針及び取扱指針

２　作業場所の報告

(1) 受託者は特定個人情報を扱う業務を行う場所（以下「作業場所」という。）を市に報告し、市の承認を得なければならない。ただし、市が作業場所を指定する場合は除く。

(2) 受託者は、(1) に定める作業場所以外で業務を行ってはならない。

３　従事者に対する教育の実施状況の報告

(1) 「適切な教育」の実施について、受託者は、情報セキュリティに対する意識の向上、個人情報の保護、本業務において業務従事者が順守すべき事項等本委託業務の適切な履行に必要な教育を、取扱責任者及び特定個人情報取扱者に対して実施しなければならない。

(2) 受託者は、(1)の教育の実施状況について、市に報告しなければならない。

(3) 「適切な教育」を受けていない者を取扱責任者又は特定個人情報取扱者とすることはできない。

４　セキュリティインシデント等の緊急事態の対応

(1) 受託者は、本委託業務に関し、セキュリティインシデント等の緊急事態が発生した場合は、その事故の発生に係る帰責の有無に関わらず、直ちに市に対して、当該事故に関わる情報の内容、件数、事故の発生場所及び発生状況を報告し、市の指示に従わなければならない。

(2) 受託者は、セキュリティインシデント等の緊急事態が発生した場合に備え、市及びその他の関係者との連絡、証拠保全、被害拡大の防止、復旧並びに再発防止の措置を迅速かつ適切に実施するための体制を整備しなければ

ならない。
(3) 市は、本委託業務に関しセキュリティインシデント等の緊急事態が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

5　提供資料の保全等

次の措置を講じなければならない。

(1) 資料等の利用者、作業場所及び保管場所の限定並びにその状況の台帳等への記録

(2) 施錠が可能な保管庫又は施錠若しくは入退室管理の可能な保管室での資料等の保管

(3) 業務従事者以外の者が本業務で取り扱う電子データにアクセスできない環境の構築

(4) 資料等を移送する場合の移送時の体制の明確化

(5) 資料等を電子データで保管する場合の、当該データが記録された媒体及びそのバックアップの保管状況に係る確認及び点検

(6) 次のセキュリティ対策を施したパソコンの利用

ⅰ　パスワード等の認証の仕組み

ⅱ　周辺機器のアクセス制限等のデータ持ち出し制限

(7) 市が所有するシステムを利用する場合、当該システムにおいて、市が指定する種類又は範囲の情報以外の情報へのアクセスの禁止

(8) 私用パソコン、私用外部記録媒体その他の私用物での作業の禁止

(9) 機密情報を含む電子データへの暗号化処理

(10) 業務に関係のないアプリケーションのインストールの禁止

(11) 海外のデータセンター等、日本の法令が及ばない場所に電子データを保管することの禁止（市が特に認める場合を除く）

(12) OS やセキュリティ対策ソフトウェアの最新状態を保持すること等による、外部からの不正アクセス防止・情報漏えい防止策の実行

(13) インターネットに接続できる環境で特定個人情報を取扱うことの禁止

(14) その他、委託の内容に応じて、提供資料の保全のために必要な措置

(15) 上記項目の従事者への周知

6　ウイルス対策

受託者は、ウイルス対策として、受託者が調達し業務処理に用いる全てのサーバ及びクライアント端末（営業担当者が用いる端末等、事務処理に用いるものを含む。）に以下の措置を講じなければならない。

(1) ウイルスの検知、リアルタイム保護、検疫機能などの機能を有するウイ

ルス対策ソフトウェアを導入すること。
(2) ウイルス対策ソフトウェアを常駐させること。
(3) パターンファイルの更新については、パターンファイルが公開された時点で迅速に適用できる仕組みを用意すること。
(4) ウイルス検出時には、利用者や情報セキュリティ担当者に迅速に通知する機能を持つと同時に、駆除・削除ができること。
(5) 毎日、曜日指定、毎週、毎月等のスケジュールを作成し、定期的にウイルスチェックを行うこと。